



National Security
and Intelligence
Review Agency

Office de surveillance des
activités en matière de sécurité
nationale et de renseignement

Office of the Privacy
Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

**NSIRA and the OPC's review
of federal institutions'
disclosures
of information under
the *Security of Canada
Information Disclosure Act*
in 2020**

© Her Majesty the Queen in Right of Canada, as represented
by the National Security and Intelligence Review Agency, 2021.
ISSN 2563-6162
Catalogue No.: PS106-10E-PDF

December 17, 2021

The Honourable Marco E. L. Mendicino, M.P.
Minister of Public Safety
269 Laurier Avenue West
Ottawa, ON K1A 0P8

Dear Minister,

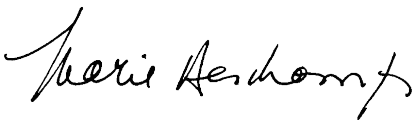
On behalf of the National Security and Intelligence Review Agency (NSIRA), it is my pleasure to present you with our second Annual Report of the *Security of Canada Information Disclosure Act* (SCIDA). As articulated in section 39 (1) of the National Security and Intelligence Review Agency Act, our report contains information with respect to the disclosures of information made under SCIDA during the previous calendar year. This review of SCIDA disclosures also took place under section 8(1)(b) of the Act, which allows NSIRA to review any activity carried out by a department that relates to national security.

This was NSIRA's first jointly coordinated review with the Office of the Privacy Commissioner (OPC) under subsection 15.1(1) of the NSIRA Act and subsection 37(5) of the *Privacy Act*. This report has benefited from our close partnership.

In accordance with paragraph 52(1)(b) of the Act, our report was prepared after consultation with the deputy heads concerned in an effort to ensure that it does not contain information whose disclosure would be injurious to national security, national defence or international relations or that is subject to solicitor-client privilege or the professional secrecy of advocates and notaries or to litigation privilege.

NSIRA and the OPC have contacted reviewed institutions for a response to the recommendations in this report and requested they provide a plan for implementation.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Marie Deschamps". The signature is fluid and cursive, with a large initial 'M' and 'D'.

The Honourable Marie Deschamps, C.C.
Chair | National Security and Intelligence Review Agency

Table of Contents

Table of Contents	3
I. Executive Summary	5
II. Authorities	7
III. Introduction	9
Background	9
SCIDA.....	9
Review Objectives.....	12
Methodology and Review Focus.....	12
IV. Findings and Recommendations	14
Disclosures of Information made under the Act in 2020.....	14
SCIDA in 2020 by the numbers	15
The primary users of the Act in 2020	15
Disclosure characteristics.....	16
SCIDA in Context	18
Example of Disclosure Outside of SCIDA Framework	19
Compliance with the Act	20
The disclosure test – Paragraph 5(1)(a).....	20
The disclosure test – Paragraph 5(1)(b).....	21
Statement of accuracy and reliability	26
Record Keeping	27
Disclosure of bulk data	29
Citizenship status checks	30
Alignment with SCIDA Guiding Principles	31
Designated Persons	31
Caveats	32
Information sharing arrangements	33
Coordination, Training, and Frameworks	35
Interdepartmental training and coordination	35
Frameworks	36
V. Conclusion	38
Timeline for implementation of recommendations	39

Annexes..... 40

Annex A: Findings and Recommendations..... 40

Findings..... 40

Recommendations 41

Annex B: Assessment of Core Policy elements by institutions..... 43

Annex C: NSIRA’s review of four disclosures of information made under SCIDA in 2019..... 46

Introduction..... 46

Authorities 46

Findings and Recommendations..... 46

I. Executive Summary

1. This report describes the results of a joint review by the National Security and Intelligence Review Agency (NSIRA) and the Office of the Privacy Commissioner (OPC) of the 215 disclosures made by federal institutions under the Security of Canada Information Disclosure Act (SCIDA or the “Act”) in 2020 – the second year of implementation of the SCIDA regime. SCIDA encourages and facilitates the disclosure of information between federal institutions to protect Canada against activities that undermine or threaten national security, subject to certain conditions.¹
2. SCIDA permits disclosures where the disclosing institution satisfies itself that the information will contribute to the exercise of the recipient institution’s jurisdiction or responsibilities in respect of activities that undermine the security of Canada², and will not affect any person’s privacy interest more than is reasonably necessary (the disclosure test)³. The review found that 212 of the 215 disclosures (approximately 99%) satisfied both parts of the disclosure test on the basis of information reviewed. All three disclosures of concern were proactive disclosures by the Royal Canadian Mounted Police (RCMP).
3. In one of the disclosures of concern, the RCMP disclosed biometric information of thousands of foreign individuals to the Department of Defence - Canadian Armed Forces (DND-CAF) based on incomplete information. Therefore, in the circumstances, the disclosure was not compliant with the requirements of SCIDA. In the other two disclosures of concern, the RCMP insufficiently demonstrated or was unable to demonstrate that they satisfied themselves that each disclosure would support the recipient in fulfilling its national security mandate. NSIRA and the OPC made related recommendations to the RCMP and DND-CAF.
4. The records reviewed also highlighted one case of a verbal disclosure made to the Canadian Security Intelligence Service (CSIS) months prior to a formal SCIDA disclosure – without an apparent source of authority for the disclosure. NSIRA and the OPC recommend that institutions with national security expertise ensure that when they request personal information for national security-related purposes from other federal institutions, they make it clear that the request, in and of itself, does not constitute or confer authority for the other institution to disclose personal information.

¹ Security of Canada Information Disclosure Act, S.C. 2015, c. 20, s. 2, [SCIDA] <https://laws.justice.gc.ca/eng/acts/S-6.9/>. SCIDA came into force on 21 June 2019. SCIDA’s predecessor, the Security of Canada Information Sharing Act, was in force from 1 August 2015 to 20 June 2019.

² SCIDA, ss. 5(1)(a)

³ SCIDA, ss. 5(1)(b)

5. SCIDA also includes provisions and guiding principles related to the management of disclosures, including accuracy statements, record keeping obligations, and information sharing arrangements.
6. With respect to accuracy statements, the review identified weaknesses in some records in relation to formulaic language, and NSIRA and the OPC recommend avoiding such language. With respect to record-keeping, the review found that the institutions had generally responsible record-keeping practices, but identified substantive weaknesses with respect to the fulsomeness of records about the information relied on by institutions to satisfy themselves of the disclosure test⁴. NSIRA and the OPC therefore make four related recommendations.
7. With respect to information sharing arrangements, based on patterns of use of SCIDA, NSIRA and the OPC recommend that the Communications Security Establishment (CSE) and Immigration, Refugees and Citizenship Canada (IRCC) enter into a formal information sharing arrangement, and that Global Affairs Canada (GAC) and CSIS update their arrangement.
8. Finally, the review also examined the frameworks institutions have in place to ensure SCIDA compliance. The review found that Public Safety Canada developed a SCIDA guide for federal institutions, leads an interdepartmental working group, and provides training. It also found that 16 of the 17 federal institutions listed in the Act – the exception being the Canadian Food Inspection Agency (CFIA) – have policies and procedures (frameworks) to support compliance with SCIDA. NSIRA and the OPC recommend CFIA develop a SCIDA framework.
9. NSIRA and the OPC are calling on the institutions to implement this report's recommendations within six months.

⁴ SCIDA, s. 9(1)(e)

II. Authorities

10. The National Security and Intelligence Review Agency (NSIRA) conducted this review under subsection 39(1) and paragraph 8(1)(b) of the *NSIRA Act*.⁵ Section 39 of the *NSIRA Act* requires NSIRA, every calendar year, to submit a report respecting the disclosure of information under the *Security of Canada Information Disclosure Act* (SCIDA or the Act) during the previous calendar year, to the Minister of Public Safety and Emergency Preparedness to be tabled in Parliament. Subsection 9(3) of SCIDA obligates all institutions that disclosed information during the year to submit records of disclosures to NSIRA, within 30 days after the end of each calendar year, for review.
11. The review was coordinated with the Office of the Privacy Commissioner (OPC) under subsection 15.1(1) of the *NSIRA Act* and subsection 37(5) of the *Privacy Act*. Subsection 37(1) of the *Privacy Act* states that the Privacy Commissioner may, from time to time at the discretion of the Commissioner, carry out investigations in respect of personal information under the control of federal institutions to ensure compliance with sections 4 to 8 of the *Privacy Act*.
12. Pertinent to the OPC's authority in this case, section 8 of the *Privacy Act* permits federal institutions to disclose personal information without the consent of the individual, under paragraph 8(2)(b), "for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure." To comply with paragraph 8(2)(b) of the *Privacy Act*, a government institution may rely on section 5 of SCIDA for authority to disclose personal information, and must comply with the requirements of SCIDA.
13. NSIRA has the legal authority to provide information to the OPC pursuant to subsection 15.1(2) of the *NSIRA Act* and the OPC has the corresponding legal authority to provide information to NSIRA pursuant to subsection 64(3) of the *Privacy Act*. During the course of the review, NSIRA and the OPC exchanged information pertaining to the review under these authorities, including records of the disclosures in question and institutions' responses to various requests for information.⁶

⁵ *National Security and Intelligence Review Agency Act*, S.C. 2019, c. 13, s. 2, <https://laws.justice.gc.ca/eng/acts/N-16.62/>

⁶ With the exception of information that was deemed by institutions to be solicitor-client privileged.

14. NSIRA and the OPC have also entered into a memorandum of understanding, which operates on the above-noted legal authorities.⁷

⁷ Office of the Privacy Commissioner. Memorandum of Understanding Regarding Coordination of Activities. June 2021. [Memorandum of Understanding Regarding Coordination of Activities - Office of the Privacy Commissioner of Canada: National](#)

III. Introduction

Background

15. This report is NSIRA's second compliance review of disclosures of information under SCIDA, and it is the first coordinated review and joint report by NSIRA and the OPC. Due to constraints caused by COVID-19, NSIRA's 2019 SCIDA report did not include an assessment of whether disclosures were legally compliant.⁸ However, NSIRA subsequently reviewed four disclosures made in 2019 as a spot check (see Annex C).
16. SCIDA was shaped by government consultations on its predecessor, the *Security of Canada Information Sharing Act* (SCISA), which was enacted in 2015. Stakeholders and the public raised concerns that SCISA would permit too much sharing of personal information, and that it lacked accountability mechanisms.⁹ In 2016, the Security Intelligence Review Committee reviewed the Canadian Security Intelligence Service's implementation of SCISA and recommended that record keeping be bolstered.¹⁰ In 2017, the OPC reviewed the operationalization of SCISA and found significant procedural deficiencies.¹¹ In part in response to these criticisms and reports, in June 2019 Parliament amended SCISA and renamed it SCIDA.

SCIDA

17. The purpose of SCIDA is to encourage and facilitate the disclosure of information *between* federal institutions to protect Canada against activities that undermine the country's security.¹² The Act does not authorize the collection of information,¹³ or the disclosure of

⁸ National Security and Intelligence Review Agency, *NSIRA's 2019 Annual Report on the Disclosure of Information under the Security of Canada Information Disclosure Act*, <https://nsira-ossnr.ca/security-of-canada-information-disclosure-act>, para 3.

⁹ Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, 2016, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-scrtr-grn-ppr-2016/index-en.aspx>; Public Safety Canada, *National Security Consultations: What We Learned Report*, 2017, <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2017-nsc-wwlr/index-en.aspx>

¹⁰ Security Intelligence Review Committee. [Impact of the Security of Canada Information Sharing Act On CSIS Information Sharing](#). August 2016.

¹¹ Office of the Privacy Commissioner. [Review of the Operationalization of the Security of Canada Information Sharing Act](#). 2017.

¹² SCIDA, s. 3

¹³ SCIDA, s. 6

information to any entities other than the 17 recipient government institutions listed in Schedule 3 of the Act.

18. Under subsection 5(1) the Act, over one hundred federal institutions may, on their own initiative or upon request, disclose information to the 17 designated federal institutions (listed in Table 1), if the institution satisfies itself that the disclosure of information:
 - a) will contribute to the exercise of the recipient institution’s jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada,¹⁴ and
 - b) will not affect any person’s privacy interest more than is reasonably necessary.¹⁵
19. The Act defines “activity that undermines the security of Canada” as any activity that:
 - Undermines the sovereignty, security or territorial integrity of Canada;
 - Threatens the lives or the security of people in Canada; or
 - Threatens the life or the security of any individual who has a connection to Canada and who is outside Canada.¹⁶

Table 1: Federal institutions that can receive information under SCIDA¹⁷

Table 1: Federal institutions that can receive information under SCIDA
1. Canada Border Service Agency
2. Canada Revenue Agency
3. Canadian Armed Forces
4. Canadian Food Inspection Agency
5. Canadian Nuclear Safety Commission
6. Canadian Security Intelligence Services
7. Communications Security Establishment
8. Department of Citizenship and Immigration
9. Department of Finance
10. Department of Foreign Affairs, Trade, and Development (Global Affairs Canada)
11. Department of Health

¹⁴ SCIDA, ss. 5(1)(a)

¹⁵ SCIDA, ss. 5(1)(b)

¹⁶ SCIDA, ss. 2(1)

¹⁷ SCIDA, Schedule 3

12. Department of National Defence
13. Department of Public Safety and Emergency Preparedness (Public Safety Canada)
14. Department of Transport
15. Financial Transactions and Reports Analysis Centre of Canada
16. Public Health Agency of Canada
17. Royal Canadian Mounted Police

20. The Act provides examples of activities that undermine the security of Canada, including “terrorism” and “espionage, sabotage or covert foreign-influenced activities.”¹⁸ Under the Act, advocacy, protest, dissent or artistic expression are not considered activities that undermine the security of Canada, unless these are carried out in conjunction with an activity that undermines the security of Canada.¹⁹
21. SCIDA also includes other requirements, notably that:
- c) under subsection 5(2), an institution that discloses information must, at the time of the disclosure, also provide information regarding its accuracy and the reliability of the manner in which it was obtained, and
 - d) under section 5.1 an institution must destroy or return any personal information received via a SCIDA disclosure, that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under lawful authority, in respect of activities that undermine the security of Canada.²⁰
 - e) under section 9, every government of Canada institution that discloses or receives information under the Act must prepare and keep records setting out certain information, and provide these records to NSIRA each year.
22. In addition, the Act’s guiding principles call for: (i) effective and responsible disclosure protects Canada and Canadians; (ii) caveats on the use of information; (iii) limits on who within an institution should receive information disclosed under SCIDA; (iv) entry into

¹⁸ SCIDA, ss. 2(1)(c) and 2(1)(d)

¹⁹ SCIDA, ss. 2(2)

²⁰ SCIDA, ss. 5.1 (3) “does not apply to the Canadian Security Intelligence Service in respect of any information that relates to the performance of its duties and functions under section 12 of the Canadian Security Intelligence Service Act.”

information-sharing arrangements where information is regularly disclosed; and (v) provision of feedback as to how disclosed information is used and useful.²¹

Review Objectives

23. The objectives of this review were to:
 - a) Assess whether disclosures and receipts of information were in compliance with SCIDA and consequently, with paragraph 8(2)(b) of the Privacy Act and whether receipts of information were in compliance with SCIDA;
 - b) Assess the extent to which the 17 designated federal institutions entered into and adhered to information sharing arrangements when they regularly used the Act to disclose or receive the same type of information; and
 - c) Assess the extent to which the 17 designated federal institutions developed and adhered to policies and procedures (frameworks), and by taking the SCIDA training session provided by Public Safety Canada.

Methodology and Review Focus

24. From January 1, 2020 to December 31, 2020, a total of 215 disclosures of information under SCIDA were reported to NSIRA. NSIRA shared these records with the OPC. NSIRA and the OPC reviewed all 215 disclosures with the related requests for information and records kept by disclosing and recipient institutions. Follow-up questions on certain disclosures were made after the initial review.
25. NSIRA and the OPC did not review the investigations or national security activities associated with the disclosures unless otherwise noted. Observations throughout the review are based entirely on the information provided to NSIRA and the OPC via requests for information and discussions with implicated institutions. Federal institutions' frameworks and information sharing arrangements were also reviewed as they were presented during the period of this review.
26. Confidence Caveat: The information provided by reviewed institutions has not been independently verified by NSIRA or the OPC. Work is underway to establish effective policies and best practices for the independent verification of various kinds of information, in keeping with NSIRA's commitment to a 'trust but verify' approach.
27. To avoid duplication, and to leverage respective expertise in assessing the requirements of Section 5 on the legal compliance of each disclosure, NSIRA led the assessment of

²¹ SCIDA, s. 4

compliance with 5(1)(a), relating to contributing to the exercise of recipients' responsibilities in respect of activities that undermine the security of Canada, whereas the OPC led the assessment of compliance with 5(1)(b), relating to the reasonable necessity of the effect on privacy interests.

IV. Findings and Recommendations

Disclosures of Information made under the Act in 2020

28. SCIDA obligates federal institutions that disclose or receive information under the Act to maintain records and to provide these records to NSIRA each year.²² In 2021, NSIRA received 215 disclosures that were made in 2020.

Table 2: List of all disclosures sent and received under the Act in 2020

Disclosing Institution	Number of Disclosures	Receiving Institution
Canada Border Service Agency	1	Canada Security Intelligence Services
Canada Border Service Agency	3	Royal Canadian Mounted Police
Global Affairs Canada	25	Canadian Security Intelligence Services
Global Affairs Canada	1	Communications Security Establishment
Global Affairs Canada	1	Immigration, Refugees, and Citizenship Canada
Global Affairs Canada	13	Royal Canadian Mounted Police
Immigration, Refugees, and Citizenship Canada	60	Communications Security Establishment
Immigration, Refugees, and Citizenship Canada	61	Canadian Security Intelligence Services
Immigration, Refugees, and Citizenship Canada	37	Royal Canadian Mounted Police
Immigration, Refugees, and Citizenship Canada	1	Transport Canada
[Institution not listed in Schedule 3 of the Act]	1	Canadian Security Intelligence Services
Transport Canada	2	Royal Canadian Mounted Police
Royal Canadian Mounted Police	3	Global Affairs Canada
Royal Canadian Mounted Police	5	Immigration, Refugees, and Citizenship Canada
Royal Canadian Mounted Police	1	Canadian Armed Forces
Total	215	

²² SCIDA, s. 9

SCIDA in 2020 by the numbers

The primary users of the Act in 2020

The primary recipients of information were the:

1. Canadian Security Intelligence Service (CSIS)

- CSIS received 88 disclosures under SCIDA in 2020.
- CSIS primarily used SCIDA to confirm or seek information about individuals under investigation or their potential associates. Requests were primarily made to Global Affairs Canada (GAC) and Immigration, Refugees and Citizenship Canada (IRCC).
- CSIS cannot use SCIDA to disclose information to other government departments.

2. Communications Security Establishment (CSE)

- CSE received 61 disclosures under SCIDA in 2020.
- CSE made 60 requests under SCIDA to Immigration, Refugees and Citizenship Canada to verify whether an individual is Canadian. These requests, all of which were responded to, related to the foreign intelligence or cybersecurity and information assurance aspects of the Establishment's mandate.²³
- While CSE may use SCIDA to disclose information to one of the 16 other designated federal institutions, to date²⁴ it has not done so.

3. Royal Canadian Mounted Police (RCMP)

- The RCMP received 55 disclosures, and made nine disclosures to other institutions under SCIDA in 2020.
- The RCMP primarily requested information under SCIDA to obtain information to support its terrorism-related investigations, including investigations relating to participation in the activity of a terrorist group.²⁵

²³ "Activities carried out by the Establishment in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations assurance aspects of its mandate must not be directed at a Canadian [...]" *Communications Security Establishment Act*, s. 22(1).

²⁴ Since SCIDA was enacted in June 2019 to the end of the reporting period of this report (December 31, 2020).

²⁵ *Criminal Code*, R.S.C., 1985, c. C-46, <https://laws.justice.gc.ca/eng/acts/C-46/index.html>, subsection 18(1), Participation in activity of terrorist group.

For the most part, these general observations are similar to those of 2019, when both CSIS and the RCMP were the main recipients of disclosures. In 2020, CSE expanded its use of the Act and received 61 disclosures of information, mostly upon request by CSE.²⁶

- The primary disclosers of information were Immigration, Refugees and Citizenship Canada (IRCC), and Global Affairs Canada (GAC), similar to 2019.
 - **IRCC was responsible for approximately three quarters of all disclosures in 2020** (159 disclosures, or approximately 74%), many of which related to information contained in **passport applications**. The purpose for these disclosures was primarily to confirm an individual’s citizenship status or to provide biographical information found on immigration application forms in order to assist an ongoing investigation or operation (in the case of CSE).
 - **GAC was responsible for almost one fifth of all disclosures in 2020** (40 disclosures, or approximately 19%), many of which contained information gathered by diplomatic missions regarding the location and movements of individuals in foreign countries. The information was primarily disclosed to assist active investigations.
- 2020 was the first time that a **federal institution outside the security and intelligence community** disclosed information under the Act.

Disclosure characteristics

- The **majority of disclosures were made upon request** (181 disclosures, or approximately 84%);
- The 34 **proactive disclosures** (approximately 16%) were primarily made by GAC and concerned information obtained through engagements in regards to consular cases.
- **Terrorism**²⁷ (89 disclosures, approximately 41%) and **espionage or covert foreign-influenced activities**²⁸ (27 disclosures, approximately 13%) were the two main activities that undermine the security of Canada observed in SCIDA disclosures in 2020.
- Federal institutions used SCIDA to disclose information about thousands of confirmed individuals and up to several thousand further individuals.

²⁶ In 2019, CSE requested five disclosures from IRCC. See: NSIRA. NSIRA’s 2019 Annual Report on the Disclosure of Information under the Security of Canada Information Disclosure Act.

²⁷ SCIDA, ss. 2(1)(d)

²⁸ The category of activity that undermines the security of Canada is “espionage, sabotage or covert foreign-influenced activity” (SCIDA, subsection 2(1)(c)). The review did not observe any disclosures related to sabotage.

- One particularly large disclosure of information related to thousands of **individuals**.
 - Another large disclosure involved several **thousand publicly available social media handles**, each potentially associated with an individual (though not necessarily, as such accounts may be automated or created by organizations rather than individuals).²⁹
 - Five other disclosures contained information on **20 individuals or more**.
 - The vast majority of disclosures related to **one or a small number of individuals**.
- The **citizenship status** of approximately 500 individuals was disclosed.³⁰ Of these individuals, over 60% were Canadians.³¹
 - Over **80%** of SCIDA disclosures **were about the suspect of an investigation or the subject of a government national security activity**.³²
 - Approximately **4% of disclosures** contained **personal information about minors**.³³
 - Approximately **15% of disclosures** made in 2020 acted as a follow-up to a **previous SCIDA disclosure** made since the Act was enacted in 2019.
 - Six disclosures (**2.8%**) were linked to **COVID-19**.³⁴
 - Eight disclosures (**3.7%**) were about an **organization**, namely, academic institutions or corporations. However, in total, these eight disclosures implicated 112 persons (one disclosure contained no personal information). The other 207 disclosures made in 2020 were about one or more individuals.

The following anonymized examples of SCIDA disclosures in Box 1 were chosen to illustrate disclosure practices that were in legal compliance with the Act. In addition to conforming with SCIDA's disclosure test, they provided evidence of discussions between institutions,

²⁹ At the time of the disclosure, the disclosing federal institution indicated to the recipient federal institution that it had removed ten records because these were "associated to Canadian citizens."

³⁰ Federal institutions are not required to identify an individual's citizenship status in SCIDA disclosures, and in many cases an individual's citizenship status is not relevant to the disclosure.

³¹ Either held Canadian citizenship, permanent resident status, or other resident status as recognized by IRCC.

³² Investigations or national security activities as conducted by the Royal Canadian Mounted Police, the Canadian Security Intelligence Service or the Communications Security Establishment.

³³ Federal institutions are not required to identify an individual's age in SCIDA disclosures.

³⁴ This information was independently identified during the course of the review and reported here, for public interest.

demonstrating that the disclosing institutions were taking steps to meet their disclosure test responsibilities under subsection 5(1) of the Act.

Box 1: Representative examples of compliant SCIDA disclosure practices made in 2020

1. IRCC disclosed information about an individual under investigation by the RCMP for financing terrorism

The RCMP sought information related to a criminal investigation of an individual suspected of financing terrorism. The RCMP requested biographical information, employment history, medical records and any other identifiable information. After an IRCC decision-maker reviewed their internal policies, IRCC disclosed less than requested, only disclosing the necessary information to assist in identifying the subject of the investigation.

2. GAC disclosed information to CSIS about a Canadian detained abroad

CSIS requested information from GAC related to a Canadian with dual-citizenship detained abroad. Prior to disclosing the information, GAC asked CSIS to further clarify the necessity of the request and the link to activities that undermine the security of Canada. CSIS did so, and GAC provided information related to consular activity with respect to the subject.

3. IRCC disclosed information to CSE on the citizenship status of an individual

CSE requested information on a person of interest. Specifically, CSE requested confirmation of Canadian citizenship or other status in Canada from IRCC. IRCC provided the result of a status check, with a caveat restricting secondary use or disclosure by CSE, as encouraged under section 4 of SCIDA.

SCIDA in Context

29. For the primary users of SCIDA – CSE, CSIS, GAC, IRCC, and the RCMP – disclosures made under the Act comprised a small portion of their domestic national security information sharing.³⁵ For example, IRCC is responsible for security screening activities under the *Immigration and Refugee Protection Act* and the *Citizenship Act* and thousands of disclosures to domestic organizations are made in a given year under those authorities.³⁶ Similarly, the RCMP discloses and receives significant amounts of information to and from other law enforcement agencies under their common law powers or other legislative authorities.³⁷ There were no disclosures from the RCMP to CSIS under SCIDA, as

³⁵ Response to NSIRA and the OPC's third request for information, received: CSE, July 19th, 2021; CSIS, July 16th, 2021; IRCC, July 20th, 2021; RCMP, July 23rd, 2021.

³⁶ Response to NSIRA and the OPC's third request for information, received: July 20th, 2021. Response #7.b.

³⁷ Response to NSIRA and the OPC's third request for information, received: July 23rd, 2021. Response #4.b. See also the RCMP's correspondence to NSIRA on 22 September 2021. Personal information may also be disclosed, for example, under paragraph 8(2)(f) of the Privacy Act.

information exchanges between the two institutions can take place under other legal frameworks.³⁸

30. However, SCIDA continues to play an important role in the sharing of national security information. Federal institutions rely on SCIDA to disclose information where other legislation or the common law does not provide an express authority to share. This appears to be the case for many users of the Act. For example, GAC indicated that SCIDA allows for the disclosure of information relating to national security where such disclosures are not explicitly provided for in the *Privacy Act*.³⁹

Example of Disclosure Outside of SCIDA Framework

31. 2020 saw the first instance of the use of SCIDA for disclosure by an institution outside the security and intelligence community (“the institution”), which was part of the intent behind the Act. This disclosure concerned a potential security risk CSIS had identified to the institution. Prior to the formal SCIDA disclosure, CSIS and the institution verbally exchanged personal information, related to the risk, and CSIS requested the institution provide it with more personal information in writing. The institution responded that it would need to check before providing more information, and two months later, CSIS proposed to the institution that it disclose under SCIDA.
32. This sequence of events raised questions as to the authority for the institution to make the verbal disclosure of personal information that occurred prior to the written SCIDA disclosure. While CSIS has authority, under the CSIS Act, to collect personal information under various circumstances, including from other federal institutions, the CSIS Act does not directly empower other institutions to disclose personal information to CSIS.
33. With respect to this specific disclosure made without apparent authority, we note that shortly after it was made, the institution proactively decided to seek advice from the Department of Justice on its disclosure authority. Its subsequent sharing of additional information (in writing) was, in our view, authorized under SCIDA. We are therefore not making further recommendations to the institution in relation to this specific incident, though we caution it to take care to establish its disclosure authority before any disclosure in future similar circumstances.
34. While this was an isolated incident amongst the 2020 disclosures that were reported to NSIRA, it highlights the importance, for all institutions, of ensuring they have lawful authority for all disclosures for national security purposes - whether it be SCIDA or another

³⁸ The RCMP and CSIS have a framework for cooperation and information sharing under their One Vision 2.0 agreement of November 2015.

³⁹ Response to NSIRA and the OPC’s second RFI, received 14 July 2021. Response #3.a.

authority. We recognize that the responsibility for ensuring disclosures are authorized ultimately rests with the disclosing institution. However, in our view, national security institutions have a role to play in fostering compliance in relation to disclosures of information that they have requested, in light of their expertise in national security matters.

Finding no. 1: The example above is illustrative that national security-related personal information can be disclosed in situations where institutions are not conscious of the requirements for lawful authority to do so.

Recommendation no. 1: In light of the restrictions under section 8 of the Privacy Act for all disclosures of personal information, NSIRA and the OPC recommend that institutions with national security expertise ensure that when they request personal information for national security-related purposes from other federal institutions, they make it clear that their requests, in and of themselves, do not constitute or confer authority for the other institution to disclose personal information.

Compliance with the Act

The disclosure test – Paragraph 5(1)(a)

35. The review found that 213 of the 215 disclosures (approximately 99%) satisfied the statutory requirement under paragraph 5(1)(a) of the Act based on the information reviewed. Paragraph 5(1)(a) of the Act requires that “the disclosure will contribute to the exercise of the recipient institution’s jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority, in respect of activities that undermine the security of Canada.”⁴⁰ In making this assessment, each disclosure and its corresponding documentation was examined to determine whether the disclosing institution had satisfied themselves that information to be disclosed fell within the recipient’s jurisdiction or would assist the recipient in its lawful authority to respond to an activity that undermined the security of Canada.
36. The review found that two disclosures were non-compliant with paragraph 5(1)(a). Both disclosures were made by the RCMP on a proactive basis to the recipient institution as opposed to in response of a request. One disclosure was received by GAC and one by IRCC. At the time of disclosure, the RCMP insufficiently demonstrated or was unable to

⁴⁰ SCIDA, ss. 5(1)(a)

demonstrate that they considered how each disclosure would support the recipient in fulfilling its national security mandate. Without this adequate consideration, the disclosures were made improperly based on a mistaken belief that disclosed information fell within the recipient’s jurisdiction. In their record-keeping to NSIRA, the RCMP was transparent and acknowledged the disclosures did not meet the requirements of the Act. As of October 2021, the RCMP was in the process of updating its SCIDA policy and practices to improve compliance with the Act.

The disclosure test – Paragraph 5(1)(b)

37. The second element of the disclosure test requires that disclosing institutions satisfy themselves that “the disclosure will not affect any person’s privacy interest more than is reasonably necessary in the circumstances.” For reasons described in detail below, the review found that most disclosures met this test. However, one non-compliant disclosure, discussed in greater detail in box two below, represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020.
38. Paragraph 5(1)(b) is in essence a proportionality test that is very similar to the minimal impairment test under section 1 of the *Canadian Charter of Rights and Freedoms* (the *Charter*) as set out in *R. v. Oakes*.⁴¹ In assessing compliance with this test, the OPC omitted from the assessment one SCIDA disclosure that, in the OPC’s view, had no impact on privacy. In this case, the disclosure did not relate to or include information about individuals (see SCIDA in 2020 by the numbers section above). However, the analysis did include 28 cases where the SCIDA disclosure was simply that the disclosing institution had no information relevant to a request received (for information about a particular individual or organization), since, in our view, even a negative response reveals personal information about the subject.
39. Consistent with the jurisprudence concerning the proportionality test under the *Charter*,⁴² in order to perform the balancing exercise, we first considered the extent of the impact on

⁴¹ In *R. v. Oakes* [1986] 1 S.C.R. 103 the Supreme Court of Canada set out the three components of the proportionality test (second branch of the *Oakes* test) for justifying a limitation on a *Charter* right under section 1 of the *Canadian Charter of Rights and Freedoms*: 1) the limit must be rationally connected to that objective; 2) the means should impair the right in question as little as possible; and 3) there must be a proportionality between the deleterious and salutary effects of the law. See articulations of the minimal impairment test in *R. v. Sharpe* [2001] 1 S.C.R. 45 para 96 and *M. v. H.*, [1999] 2 S.C.R. 3 at para 118.

⁴² When performing the proportionality analysis under *Oakes*, the Supreme Court has considered the impact on the *Charter* right, the seriousness of a particular limit, and how substantial or significant the limitation was (see for example, *Law Society of British Columbia v. Trinity Western University*, [2018] 2 S.C.R. 293 at paras 80-88 and *Alberta v. Hutterian Brethren of Wilson Colony*, [2009] 2 S.C.R. 567 at paras 88-91.

the individual’s privacy interest for the 214 disclosures where there was an impact on privacy. The factors considered included the universal privacy considerations of sensitivity, vulnerability of the individuals, and how the information could be used. Additionally, in a national security context, the assessment of the impact on privacy interests must also consider the privacy effect of national security use itself. One relevant element the OPC considered was whether, in searching for individuals of interest, there were any disclosures of large data sets to a national security agency that included many individuals with no apparent connection to a national security matter. This could have a significant undermining effect on individuals’ sense of privacy with respect to the extent of government intrusion in their lives, even if no action is taken against them directly.

40. Using the considerations above, we assessed that privacy impact of these disclosures on a scale of low, medium, high, or very high:

Impact	Description of privacy effect	Number	Percentage
Low	Potential harm to individuals life, safety, liberty, property, finances, reputation or other privacy interests is minimal or relatively low and/or likely remediable. ⁴³	117	54.7%
Medium	Potential harm to individual(s) life, safety, liberty, property, finances, reputation or other privacy interests is moderate and/or may be remediable in whole or in part.	85	39.7%
High	Potential harm to individual(s) life, safety, liberty, property, finances, reputation or other privacy interests is significant and/or likely not remediable.	11	5.1%
Very High	Potential harm to individual(s) life, safety, liberty, property, finances, reputation or other privacy interests is severe or irreversible.	1 ⁴⁴	0.5%

41. With respect to the privacy effect of national security use, it was encouraging that most of the disclosures were targeted disclosures in relation to one or a small number of individuals, and that disclosing institutions included caveats such as conditions on secondary use. These are all indications that privacy impacts were minimized. In the cases where larger datasets were disclosed, the individuals included all had, at a minimum, a

⁴³ Where more individuals were affected, the privacy effect was assessed as elevated for all categories of impact.

⁴⁴ This single case included information about thousands of individuals. See below for further details.

suspected connection to activities undermining the security of Canada, which was another positive indication.

42. The OPC then assessed whether the privacy interest was impacted more than was ‘reasonably necessary’ in the circumstances. Specifically, the OPC considered the objective of each disclosure, in light of the purpose of SCIDA,⁴⁵ and where a request was made, if it was broad or precise in nature. The OPC considered whether a meaningful disclosure could have been made with some of the information omitted or if there were any alternatives available that affected the privacy interest any less. For cases with a significant privacy impact, the assessment also entailed a review of the records kept, and any follow-up inquires, to determine whether or not the disclosing institution took reasonable steps to mitigate the privacy impact, such as attempting to narrow the scope of the request and/or redacting or withholding extraneous information not reasonably necessary to achieve the objective of the disclosure. In almost all cases, the OPC found that the disclosures met the test of not affecting privacy interests more than was reasonably necessary in the circumstances.
43. It appears that there are well-established relationships between several of the implicated institutions that predate the enactment of both SCISA and SCIDA. Consistent with the findings with respect to compliance with the first part of the disclosure test,⁴⁶ the disclosure of information between the five primary institutions that disclose and receive information under SCIDA – CSE, CSIS, IRCC, GAC, and the RCMP – seems to be routine.
44. Positive indications of the limits of requests were found in CSE’s 60 requests for information from IRCC, where CSE was careful to seek only to determine particular individuals’ citizenship or immigration status (to avoid directing their activities at Canadians), and IRCC was in turn careful to disclose only a minimal amount of information regarding citizenship and nothing more.
45. IRCC, which made the majority of the SCIDA disclosures in 2020, was also able to demonstrate, during the course of the review, that its internal SCIDA policy requires its analysts to consider, on a case-by-case basis for every SCIDA disclosure, each individuals’ privacy interests in order to assess compliance with the disclosure test. The policy also requires each analyst to complete a thorough assessment before making a disclosure. In some cases IRCC had redacted some information, while in other cases, it responded that it located additional information about the subject individual(s) but deemed that information to be non-responsive to the request. In one case, IRCC noted that it refused entirely to provide a disclosure in response to a request that was inadequately formulated. The OPC is

⁴⁵ Section 3 of SCIDA (Purpose clause).

⁴⁶ SCIDA, ss. 5(1)(a)

therefore satisfied that IRCC appears to be correctly assessing necessity and proportionality on a case-by-case basis prior to disclosing personal information under SCIDA.

46. As another example, GAC made a total of 37 disclosures to CSIS (24) and the RCMP (13). The OPC notes that in all of these cases the information that was disclosed related specifically to diplomatic matters and responded precisely to the requests from CSIS and the RCMP without disclosing extraneous personal information that would not have been reasonably necessary.
47. However, as noted above, the OPC identified some areas of concern:

Box 2: Key disclosures reviewed in greater detail due to sensitivity and volume

1. GAC proactive disclosure of a list of several thousand publicly available social media handles to CSE

The OPC noted that there was only very limited information on file to support the purpose of this particular disclosure, which consisted of an extensive list of social media handles, each potentially associated with an individual (though not necessarily, as social media handles may be automated or created by organizations rather than individuals). The list was provided proactively to CSE for the purpose of tracking social media handles that were thought to be spreading disinformation with respect to the COVID-19 pandemic, which could impact the security of Canada. While the social media handles themselves may not represent individuals' real identities, there are likely individuals associated with at least some of the handles, whose privacy interests are therefore at play – in the context of being included in a list of handles suspected of maliciously spreading disinformation.

In response to our questions, GAC explained the disclosure in more detail, including that the list had been created using only publically available information associated with social media handles – and included only handles identified as potentially engaged in malicious spreading of disinformation. The OPC ultimately accepted that in this context, despite the high volume of handles involved, any effect on the privacy interests of individuals associated with the handles was not more than was reasonably necessary in the circumstances.

2. RCMP proactive disclosure to the Department of Defence - Canadian Armed Forces (DND-CAF)

Biometric information of thousands of men, women and children, detained by a third party on suspicion of being members or supporters of a terrorist organization, was provided to the RCMP by a trusted foreign partner. The RCMP then proactively disclosed the same information to DND-CAF pursuant to SCIDA, with the exception of a small number of records about Canadians. The RCMP indicated that it was providing the information to DND-CAF in light of DND-CAF's counter-terrorism mandate and active operations in the region in which the individuals were detained. On this basis we accept that the RCMP satisfied itself that the 5(1)(a) disclosure test was met.

Given that the information was biometric information, accompanied by the suspicion of terrorism, the effect on the privacy interests of the detained individuals from the disclosure is very high. We therefore examined how the RCMP satisfied itself that the disclosure did not affect any person's privacy interest *more than reasonably necessary in the circumstances*. The dataset received from the

trusted foreign partner was accompanied by a message indicating that a detailed description of the dataset would follow. The detailed description included contextual information about how the information was obtained and specific caveats on its use, which could have a bearing on DND-CAF's use of the dataset. However, it came to light that when the RCMP decided to disclose the information to CAF approximately eight months later, it had no record of having received this detailed description and did not seek a copy from the originator until our review. In our view, the missing information would have been necessary to properly assess both the effect on privacy interests and the reasonable necessity of the disclosure. Therefore, the RCMP could not have satisfied itself that paragraph 5(1)(b) of SCIDA was met. Consequently, the disclosure contravenes section 5(1)(b) of the Act.

The RCMP gave a similar but less explicit caveat on use of the information to DND-CAF. However, the detailed caveat and contextual information was not provided to DND-CAF. This is despite an assurance that the information was being provided in the exact manner received, except for the removal of the information of Canadians.

If the RCMP were to reassess the disclosure in light of the full contextual information, informed by related discussions with DND-CAF, it is unclear if the disclosure would meet 5(1)(b) of SCIDA in light of DND-CAF's associated biometric policies and directives.

DND-CAF indicated that in the fifteen months since receiving the information it had not used or integrated it into its systems, but that it needed to retain the information for force protection and to rapidly identify threats. We are making a related recommendation below to DND-CAF to reassess.

48. In addition to the contravention above (#2 in Box 2), NSIRA and the OPC also found that in the cases identified in the previous section as not meeting part (a) of the disclosure test, part (b) of the disclosure test was also not met. Disclosures that do not contribute to the recipient institution's responsibilities in respect of activities that undermine the security of Canada and could affect a person's privacy interest will, by definition, affect a person's privacy interest more than is reasonably necessary in the circumstances. Notably, the disclosure in one of these two cases did not relate to any individuals.
49. This leaves two disclosures, of the total of 215, where the disclosures affected individuals' privacy interests more than was reasonably necessary in the circumstances. Both were made by the RCMP.⁴⁷
50. One of these disclosures represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020. This highlights that it is important that decision makers empowered to make SCIDA disclosures understand the necessity to have fulsome information to confidently assess whether the disclosure test is met.

⁴⁷ IRCC destroyed the personal information it received from the RCMP in the non-compliant disclosure to IRCC.

Finding no. 2: NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020 satisfied the disclosure test under paragraph 5(1)(a) based on information reviewed.

Finding no. 3: NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020, appear not to affect any persons' privacy interest more than was reasonably necessary in the circumstances based on information reviewed. However, one non-compliant disclosure by the RCMP represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020.

Recommendation no. 2: NSIRA and the OPC recommend that the RCMP finish updating its SCIDA policy to support compliance with the disclosure test in the Act, and provide guidance to its decision-makers empowered to make SCIDA disclosures on the analysis required to satisfy themselves that the disclosure test is met; and, ensure that these decisions are properly documented.

Recommendation no. 3: First, NSIRA and the OPC recommend that the RCMP provide fulsome information about the non-compliant disclosure to DND-CAF. Second, NSIRA and the OPC recommend that consistent with section 5.1 of SCIDA, DND-CAF assess the necessity of retaining the personal information received in light of this new information, our findings, associated DND-CAF directives⁴⁸ and other applicable policies.⁴⁹

Statement of accuracy and reliability

51. Disclosing institutions are required, under subsection 5(2) of the Act, to provide information regarding the accuracy of information disclosed and the reliability of the

⁴⁸ Including, Canadian Armed Forces. Chief Of Defence Intelligence Interim Functional Directive: Guidance on the Collection, Use, Handling, Retention and Disclosure of Biometric Data during Expeditionary Operations.

⁴⁹ Section 5.1. of SCIDA requires that an institution destroy or return any personal information received via a SCIDA disclosure, that is not necessary for the institution to exercise its jurisdiction, or to carry out its responsibilities, under lawful authority, in respect of activities that undermine the security of Canada.

manner in which it was obtained. These statements contribute to the utility of disclosed information as it provides valuable context to the receiving institutions.

52. Nearly all disclosures included accuracy and reliability statements, although there were inconsistencies. Certain institutions that hold and share information that is received through standard processes, such as passport applications, can more reliably use formulaic language as this is generally the only information that they have before them. Institutions that gain information through other, less routine means such as in-person interviews, may require more specificity in their statements. For example a statement on the accuracy and reliability strictly referencing the manner in which it was obtained may introduce a false perception that an interviewee's statements are similarly accurate and reliable. In the RCMP proactive disclosure to DND-CAF (outlined in Box 2), the statement of accuracy and reliability contained incomplete information and did not include all of the relevant details provided by the trusted foreign partner.

Finding no. 4: Almost all of the disclosures (nearly 98%) included accuracy and reliability statements, although there were inconsistencies with respect to the sufficiency and specificity of statements.

Recommendation no. 4: NSIRA and the OPC recommend that the federal institutions listed in the Act avoid formulaic language in statements of accuracy and reliability when the nature and source of information disclosed is not derived from a routine process.

Record Keeping

53. All federal institutions that disclose information under SCIDA are required, under section 9 of the Act, to prepare and keep records of information that is disclosed or received and submit them to NSIRA annually. The Act details the type of information to be recorded in institutional records. The records by the disclosing institutions must include: (i) a description of the information; (ii) the name of the recipient institutions, (iii) the individual who authorized the disclosure; (iv) the date on which it was disclosed; and (v) a description of the information that the disclosing institution relied on to satisfy itself that the disclosure was authorized under the Act. Similar record keeping requirements apply to the receiving institution.
54. NSIRA and the OPC found that eight of nine federal institutions that disclosed or received information under the Act in 2020 prepared and kept records of disclosures and receipts. The records of a given calendar year must be provided to NSIRA annually, by January 30th

of the following year. NSIRA found that all of the eight institutions listed in the Act that disclosed or received information under SCIDA in 2020 provided their records by the statutory deadline. The record keeping of the ninth institution, that made a single disclosure to CSIS for the first time, did not meet the record-keeping requirements as set out in the Act. Our review found that the institution did have reasonably fulsome documentation pertaining to the disclosure, but that it was unaware of the specific record-keeping requirements (and the related requirement to submit to NSIRA). This may be because the institution is not listed in the Act and is not a member of the security and intelligence community.

Finding no. 5: The record keeping of one institution which used SCIDA for the first time did not meet the record-keeping requirements of the Act.

Recommendation no. 5: NSIRA and the OPC recommend that institutions listed in Schedule 3 of the Act that request information from institutions not listed in SCIDA, inform the disclosing institution of their legal obligations with respect to disclosing information under the Act, including record-keeping requirements, and encourage the disclosing institution to seek advice from Justice Canada and Public Safety Canada.

55. The institutions that did keep records and provide these to NSIRA displayed generally responsible record keeping. Most were well organized with no discrepancies. Still, certain requests were provided in an a disorganized manner that required significant examination to associate them with their disclosures, which made the review process more difficult, and in one case two disclosures were given the same file name. While these records still met the requirements of the Act, they were difficult to understand and review. More standardized record-keeping would render the records more useful for both internal and external reporting purposes, and would help institutions and NSIRA identify gaps and areas for improvement.

Finding no. 6: Most records were well organized with no discrepancies, although some were provided in a manner that was difficult to understand and review.

Recommendation no. 6: NSIRA and the OPC recommend that federal institutions that routinely disclose or receive in accordance with the Act standardize their record keeping in accordance with the latest Public Safety guidance.

56. The most serious concerns we had with respect to contents of the records related to the requirement under paragraph 9(1)(e) to keep a description of the information the disclosing institution relied on to satisfy itself that the disclosure was authorized under the Act. In the cases described in the previous section where the disclosure test under paragraph 5(1)(b) of the Act was not demonstrated to be met, the related records were overly brief on the rationale for the disclosure. In the one RCMP disclosure that accounted for the vast majority of the personal information disclosed, the records of both parties were based on incomplete information. Additionally, when the RCMP submitted its records to NSIRA, they identified five proactive disclosures where contemporaneous record keeping was not done. Their annotations and self-identification of this issue provided sufficient information that the disclosure was authorized by SCIDA.
57. We found that most of the inadequate records under 9(1)(e) were found in two types of disclosures: bulk information disclosures, and routine disclosures made with limited case-by case documentation – such as for citizenship status checks.

Disclosure of bulk data

58. Certain disclosures contained information on over 50 people, with one such disclosure containing information on thousands of individuals, and a second containing information associated with up to 6844 individuals. Potential privacy concerns are amplified when bulk data is shared given the sheer volume of information. As most SCIDA disclosures consist of personal information, bulk data – especially novel databases that contain personal information – should be shared with additional scrutiny and care.
59. SCIDA section 9(1)(e) states that SCIDA disclosure records must contain “a description of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act.” As noted in the previous section, we examined the bulk disclosure above in more detail. In both of the largest disclosures made (see Box 2 above) the SCIDA records submitted to NSIRA did not include an adequate description of the information used to support the disclosing institution’s determination that the disclosure was authorized, commensurate to the volume and privacy interests in the information disclosed.

60. Further, we note there is greater risk with regards to the misuse or mislabeling of information when shared in bulk. Federal institutions should therefore have frameworks in place for sharing of this type of bulk data to satisfy themselves that all requirements of the Act have been met, including using precise caveats and statements of accuracy and reliability. When responding to requests for information for bulk datasets, institutions should minimize the sharing of extraneous data.

Citizenship status checks

61. All 60 of CSE's requests for information to IRCC regarding the citizenship status of an individual contained identical language that did not identify the activity that undermines the security of Canada for which the request was being made. As the disclosing institution, the burden of responsibility rests with IRCC to ensure they had sufficient grounds to disclose under SCIDA. IRCC confirmed that discussions which identified CSE's general requirement for the verification of citizenship (to avoid directing its activities at Canadians, which would be contrary to the *CSE Act*) had transpired prior to the first disclosure of this information. However, the particular activities that undermine the security of Canada that each disclosure request related to, were not specifically identified in the subsequent requests.⁵⁰
62. In contrast, CSIS provided fulsome details in its requests to GAC for information under SCIDA. CSIS explained that under an information sharing arrangement with GAC relating to SCIDA's predecessor, SCISA, GAC had set a high threshold for information it required to assess requests for information. Therefore, CSIS provides detailed information to aid in GAC's assessment, including details of the potential impact on the subject(s) of the request, as well as to verify identities of subjects and assist GAC in reporting on accuracy of information disclosed (as required under subsection 5(2) of SCIDA). Consequently, GAC's records describing the information it used to satisfy itself that the disclosures to CSIS met the disclosure test in section 5 were exemplarily robust.

Finding no.7: This review found instances where records kept for disclosures did not contain a sufficient description, as required under paragraph 9(1)(e), of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act.

⁵⁰ SCIDA, ss. 9(e)

Recommendation no. 7: NSIRA and the OPC recommend that institutions ensure that records kept for bulk disclosures include an appropriately robust description of the information relied on to satisfy itself that the disclosure of *all* elements of the dataset meets section 5 of the Act, and that the level of internal oversight is commensurate with the privacy risk.

Recommendation no. 8: NSIRA and the OPC recommend that federal institutions include information about how the disclosure will contribute to their jurisdiction or responsibilities in respect of activities that undermines the security of Canada, and other information relevant to the disclosure test, in their written requests for information under the Act, even if this information was verbally communicated prior to the request to enable appropriate record keeping by disclosing institutions under SCIDA.

Alignment with SCIDA Guiding Principles

Designated Persons

63. SCIDA includes, as a guiding principle, that “only those within an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities that undermine the security of Canada ought to receive information that is disclosed under this Act.”⁵¹ Subsection 5(1) also indicates that disclosures are to be made to the head of a recipient Government of Canada institution whose title is listed in Schedule 3, or to a person designated by the head of that recipient institution.
64. NSIRA found that all 17 federal institutions that receive information under the Act had designated persons for this purpose, as required by the Act.⁵² Under SCIDA, there is no requirement for institutions to designate persons to receive disclosures as the head of an institution can receive information by default. Still, designation facilitates the timely and reliable transfer of information as observed by NSIRA and the OPC in this review.
65. With the exception of the CBSA and CSIS, the federal institutions that designated persons under the Act designated a small number of executives or managers. CSIS designated employees in certain operational units and sub-units. CBSA also designated classes of employees, including managers in the Operations branch at national headquarters,

⁵¹ SCIDA, ss. 4(e)

⁵² SCIDA, ss. 5(1)

intelligence and enforcement officers at the agency's National Border Operations Centre, and all of its Liaison Officers internationally.

66. Designating classes of employees who work in relation to activities that undermine the security of Canada is an acceptable practice, and is appropriate given the mandates and structures of CBSA and CSIS. Other federal institutions that wish to consider designating classes of employees must similarly do so with regard to their specific mandate and structure. The CBSA's policy states that in urgent or exigent circumstances, CBSA officials with a role in border operations or intelligence – including Border Service Officers – may request or receive information under the Act even if they are not within the above-noted designated classes. “These rare situations must be handled on a case-by-case basis, and proper recording procedures must be followed and applied (retroactively) as soon as possible.”⁵³ Expanding access may provide flexibility in responding to urgent or exigent circumstances, and is appropriate for CBSA officials with a role that involves addressing activities that undermine the security of Canada.
67. NSIRA was encouraged that CBSA had considered urgent and exigent circumstances in their implementation of the Act, and encourages the other federal institutions listed in SCIDA to do the same.

Caveats

68. SCIDA includes, as a guiding principle, that “respect for caveats on and originator control over disclosed information is consistent with effective and responsible disclosure of information.” The review found that institutions included caveats on over 96% of disclosures. Caveats place limits on how information can be used by the recipient institution. This is encouraged by the Act⁵⁴ because it supports originator control and responsible information sharing. For example, a caveat may prohibit the recipient institution from disclosing the information further without the express permission of the disclosing institution, or it may ask a law enforcement agency such as the RCMP to not use the information in a criminal proceeding without notifying the originator. To promote greater consistency, NSIRA encourages federal institutions to set out the exact wording of caveats in policy and to develop caveats in consultation with the Department of Justice.

⁵³ Canada Border Services Agency, *Directive on Sharing Information Pursuant to the Security of Canada Information Sharing Act (SCISA)*, 12 August 2015, p. 15, bold emphasis removed, parenthesis in original. CBSA issued this directive in for SCIDA's predecessor (SCISA) and now uses it for SCIDA.

⁵⁴ SCIDA, ss. 4(b)

Finding no. 8: NSIRA and the OPC found that almost all disclosures (over 97%) included caveats, which supported originator control and responsible information sharing.

Information sharing arrangements

69. A further guiding principle in Section 4 of SCIDA is that entry into an information sharing arrangements (ISA) is appropriate when a federal institution regularly discloses information under the Act to the same institution.⁵⁵ The Act does not limit this guidance to the federal institutions listed in the Act.
70. In guidance published by the Treasury Board of Canada Secretariat, the establishment of ISAs are recommended as a measure to “outline the terms and conditions under which personal information is shared between [...] parties.”⁵⁶ ISAs provide a framework to determine whether personal information should be shared in a legally compliant manner, and how best to do so.

Information-Sharing Arrangements provided to this review included:⁵⁷

- CBSA has information-sharing arrangements with CSIS, IRCC and the RCMP.
- The CRA and the RCMP concluded a memorandum of understanding in 2012, which covers information sharing between the two institutions. The CRA and the RCMP are working towards a new memorandum of understanding that expressly mentions SCIDA.
- CSIS and GAC concluded an information-sharing arrangement under SCIDA’s predecessor legislation in 2016. This information-sharing arrangement is used for disclosures of information under SCIDA. We note that in response to questions we posed to CSIS about disclosures from GAC to CSIS, there were internal concerns that the implementation of the agreement was inconsistent. The coming into force of SCIDA in 2019, with a higher two-part threshold, provides an opportunity to revisit this arrangement and ensure common understanding between the organizations

⁵⁵ SCIDA, ss. 4(c)

⁵⁶ Treasury Board of Canada Secretariat. *Guidance on Preparing Information Sharing Agreements Involving Personal Information*. July 2010. <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html>

⁵⁷ NSIRA and the OPC did not assess whether federal institutions adhered to their internal policies for the drafting of information sharing arrangements.

71. In 2020, IRCC regularly disclosed information about individuals' citizenship status to CSE. This was done under SCIDA and not under another lawful authority, and it appears to be a new, ongoing and regular practice for these two institutions. An information sharing arrangement between the two institutions would align with the principles set out in SCIDA and lay the foundation for an increase in responsible information sharing which would be beneficial to CSE carrying out its mandate.
72. IRCC's policy on SCIDA states that "IRCC usually requires an ISA when information is being shared on a systematic or recurrent basis, but an ISA could also be desired for situations when a large volume of information is being shared on an ad hoc basis or when it involves sensitive personal information. The Treasury Board Secretariat's *Guidance on Preparing Information Sharing Agreements Involving Personal Information* is a useful tool to use in the consideration and development of ISAs."⁵⁸ NSIRA and the OPC agree. CSE stated that it began drafting an ISA with IRCC two years ago, but had placed it on hold after being informed that Public Safety Canada was working towards an ISA template for federal institutions.⁵⁹

Finding no. 9: IRCC and CSE, as well as GAC and CSIS, regularly exchange information under SCIDA of a nature and in a manner that warrants information sharing arrangements, as encouraged by subsection 4(c) of the Act.

Recommendation no. 9: NSIRA and the OPC recommend that IRCC and the CSE enter into an information-sharing arrangement that structures their disclosure of information under the Act.

Recommendation no. 10: NSIRA and the OPC recommend that CSIS and GAC update their information-sharing arrangement, previously agreed upon under SCISA, to account for SCIDA.

⁵⁸ Immigration, Refugees and Citizenship Canada, Immigration, Refugees and Citizenship Canada Policy on Information Sharing under the Security of Canada Information Disclosure Act, 12 May 2020, p. 14.

⁵⁹ CSE response to NSIRA consultation on SCIDA 2020 review, draft report and recommendations. September 21st, 2021.

Coordination, Training, and Frameworks

Interdepartmental training and coordination

73. Public Safety Canada plays a leadership role in the federal government's use of SCIDA. In 2019, Public Safety Canada's Strategic Coordination Centre on Information Sharing founded the National Security Information Sharing Interdepartmental Working Group. The Working Group provides policy leadership, guidance and support to federal institutions on responsible information sharing practices to foster increased collaboration and integration between federal institutions with national security mandates.
74. In December 2019, the Strategic Coordination Centre on Information Sharing produced the *SCIDA Step-by-Step Guide to Responsible Information Sharing*. This is a detailed guide for federal institutions on how to use the Act, and includes checklists for the disclosure and receipt of information and for record-keeping. The guide also lists the national security mandates of the 17 federal institutions listed in the Act and the officials designated in each institution to receive information under the Act. As of July 2021, the Strategic Coordination Centre on Information Sharing was working with the National Security Information Sharing Interdepartmental Working Group to produce the next version of the *SCIDA Step-by-Step Guide to Responsible Information Sharing*.
75. From the coming into force of SCIDA in June 2019 to August 2021, the Strategic Coordination Centre on Information Sharing trained 515 individuals at 33 federal institutions, including all 17 federal institutions listed in the Act.
76. This training included the participation of federal institutions not listed in the Act. Part of the intent behind SCIDA is for federal institutions not in the security and intelligence community to be able to disclose information to the federal institutions that are listed. As the use of SCIDA expands in future years, increased awareness of the Act will be necessary for a larger number of institutions to disclose information under the Act.
77. Institutions unfamiliar with SCIDA that receive requests from those listed in the Act should educate themselves on its appropriate use and their institutional responsibilities. Public Safety Canada's training and guide comprise important foundational knowledge regarding responsible information disclosure. Institutions listed in the Act should make themselves available as valuable resources to the uninitiated. As the burden of responsibility for certain key aspects of compliance are placed on the disclosing institution, requesting institutions, and specifically their legal counsel, should be forthcoming in sharing their knowledge and experience with SCIDA.

Finding no. 10: NSIRA and the OPC found that Public Safety Canada coordinates the implementation of SCIDA among federal institutions, and that all 17 federal institutions listed in SCIDA have staff who have taken Public Safety Canada’s SCIDA training.

Frameworks

78. NSIRA expected the 17 federal institutions listed in the Act to have implemented frameworks (namely, policies and procedures) related to SCIDA. Frameworks support compliance with the law, manage operational and legal risks, and support consistency and accountability.
79. 16 of the 17 federal institutions listed in SCIDA⁶⁰ have frameworks to govern information sharing under the Act. For many of these 16 federal institutions, their framework consists entirely or almost entirely of Public Safety Canada’s *SCIDA Step-by-Step Guide to Responsible Information Sharing*.⁶¹
80. The institution without a SCIDA framework is the CFIA. The CFIA has never disclosed or received information under SCIDA. Still, having a framework institutionalizes the Act to ensure that when a need to engage SCIDA arises, a sufficient framework will exist within the institution to do so.
81. In addition, while CSIS has a SCIDA framework – consisting of the *SCIDA Step-by-Step Guide to Responsible Information Sharing* and a bulletin for employees about the coming into force of SCIDA – in June 2021 the Service indicated it was in the process of updating its internal policy from SCISA (the predecessor to SCIDA) to SCIDA.
82. The RCMP is also in the process of reviewing its existing SCIDA framework.⁶²

Finding no. 11: NSIRA and the OPC found that the Canadian Food Inspection Agency did not have policies or procedures to support compliance with the Act.

⁶⁰ SCIDA, Schedule 3

⁶¹ Public Safety Canada, *Security of Canada Information Disclosure Act (SCIDA): A Step-by-Step Guide to Responsible Information Sharing*, December 2019, 92 pages, *SCIDA Step-by-Step Guide to Responsible Information Sharing* hereafter.

⁶² Royal Canadian Mounted Police. *Standard Operating Procedures (SOPs) for Handling Requests Made Pursuant to the Security of Canada Information Disclosure Act (SCIDA)*. Received by NSIRA in January 2021.

Recommendation no. 11: NSIRA and the OPC recommend that the Canadian Food Inspection Agency consult Public Safety Canada, and develop and implement policies and procedures to support compliance with the Act.

83. Finally, NSIRA remains cognizant that frameworks alone will not ensure information is disclosed responsibly and with the necessary safeguards. For those institutions that regularly use the Act to repetitively disclose information of a similar kind, it is imperative they remain attentive to the unique circumstances surrounding each individual disclosure. Caveats, the disclosure test, and accuracy and reliability statements should all be applied with precision and to meet the specific needs of a disclosure.
84. Annex B summarizes NSIRA's assessment of federal institutions' SCIDA frameworks against certain requirements of the Act. This annex tabulates what is in policy and not what occurred in practice.

V. Conclusion

85. Our review found that in SCIDA's second year of use, 212 of the 215 disclosures were compliant with the Act. However, one single non-compliant disclosure by the RCMP accounted for the vast majority of confirmed individuals affected by SCIDA disclosures in 2020. Given the ability for SCIDA to be used for proactive bulk disclosures of personal information, it is critical that each disclosure be carefully analyzed against the disclosure test, and that institutions can demonstrate, in their records, how, concretely, the test was met.
86. For certain institutions, information sharing under the Act has become routine, with policies and practices in place to ensure legal compliance and diminish adverse privacy impacts. However, the repetitive nature of request and disclosure lends itself to inattentive missteps, and it is vital that institutions apply their frameworks with rigour in each unique instance of disclosure or receipt. Improvements to record-keeping to meaningfully document the application of this rigour as required by the Act are a key part of ensuring continued due diligence. This expectation of institutionalization is not only to be applied to the major requesting and disclosing institutions under the Act, but to all users, even those who use the Act infrequently.
87. Institutions identified as primary users of the Act, which have established and tailored frameworks, should also make themselves available to provide guidance to domestic partners. Best practices should be shared, and while the training materials prepared and disseminated by Public Safety Canada provide a strong foundation, institutions can provide additional insight on the implementation of frameworks and diligence with regards to record keeping.
88. Notably, 2020 saw the first instance of an institution not listed in the Schedule 3 of the Act using the Act to disclose information. As the use of SCIDA expands, more institutions inexperienced with engaging the Act will begin to do so. It is therefore important that all Government of Canada institutions have access to and benefit from Public Safety Canada's resources and training. This first instance highlighted not only the challenges associated with ensuring SCIDA obligations such as record keeping are met by occasional users of SCIDA, but also brought to light an instance of a national-security related disclosure outside the SCIDA framework with no apparent authorization. This is a key reminder that the SCIDA framework only provides meaningful checks and balances on disclosures made within it. National security institutions have a key role to play in ensuring that disclosures requested from other institutions are grounded in lawful authority, be it SCIDA or otherwise.

89. This joint review assessed 215 disclosures of information for legal compliance and privacy impacts. Future reviews may take a more narrow approach, for example, by examining the reasonableness and necessity of specific requests and disclosures as they relate to the underlying investigation or operation. NSIRA and the OPC encourage institutions to continue to develop and institutionalize SCIDA frameworks, seek out and share best practices, and implement the recommendations of this review (listed in Annex A) in a timely way.

Timeline for implementation of recommendations

90. NSIRA and the OPC call on the reviewed institutions to implement this report's recommendations within six months of receiving this report.

Annexes

Annex A: Findings and Recommendations

Findings

1. The example above is illustrative that national security-related personal information can be disclosed in situations where institutions are not conscious of the requirements for lawful authority to do so.
2. NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020 satisfied the disclosure test under paragraph 5(1)(a) based on information reviewed.
3. NSIRA and the OPC found that almost all (approximately 99%) of the disclosures of information made under the Act in 2020, appear not to affect any persons' privacy interest more than was reasonably necessary in the circumstances based on information reviewed. However, the one non-compliant disclosure by the RCMP represents the vast majority of all confirmed personal information that was disclosed under SCIDA in 2020.
4. Almost all of the disclosures (nearly 98%) included accuracy and reliability statements, although there were inconsistencies with respect to the sufficiency and specificity of statements.
5. The record keeping of one institution which used SCIDA for the first time did not meet the record-keeping requirements of the Act.
6. Most records were well organized with no discrepancies, although some were provided in a manner that was difficult to understand and review.
7. This review found instances where records kept for disclosures did not contain a sufficient description, as required under subsection 9(1)(e), of the information that was relied on to satisfy the disclosing institution that the disclosure was authorized under this Act.
8. NSIRA and the OPC found that almost all disclosures (over 97%) included caveats, which supported originator control and responsible information sharing.
9. IRCC and CSE, as well as GAC and CSIS, regularly exchange information under SCIDA of a nature and in a manner that warrants information sharing arrangements, as encouraged by subsection 4(c) of the Act.
10. NSIRA and the OPC found that Public Safety Canada coordinates the implementation of SCIDA among federal institutions, and that all 17 federal institutions listed in SCIDA have staff who have taken Public Safety Canada's SCIDA training.

11. NSIRA and the OPC found that the Canadian Food Inspection Agency did not have policies or procedures to support compliance with the Act.

Recommendations

1. In light of the restrictions under section 8 of the Privacy Act for all disclosures of personal information, NSIRA and the OPC recommend that institutions with national security expertise ensure that when they request personal information for national security-related purposes from other federal institutions, they make it clear that their requests, in and of themselves, do not constitute or confer authority for the other institution to disclose personal information.
2. NSIRA and the OPC recommend that the RCMP finish updating its SCIDA policy to support compliance with the disclosure test in the Act, and provide guidance to its decision-makers empowered to make SCIDA disclosures on the analysis required to satisfy themselves that the disclosure test is met; and, ensure that these decisions are properly documented.
3. First, NSIRA and the OPC recommend that the RCMP provide fulsome and accurate information to DND-CAF about the non-compliant disclosure. Second, NSIRA and the OPC recommend that consistent with section 5.1 of SCIDA, DND-CAF assess the necessity of retaining the personal information received in light of this new information, our findings, associated DND-CAF directives and other applicable policies.
4. NSIRA and the OPC recommend that the federal institutions listed in the Act avoid formulaic language in statements of accuracy and reliability when the nature and source of information disclosed is not derived from a routine process.
5. NSIRA and the OPC recommend that institutions listed in Schedule 3 of the Act that request information from institutions not listed in SCIDA, inform the disclosing institution of their legal obligations with respect to disclosing information under the Act, including record-keeping requirements, and encourage the disclosing institution to seek advice from Justice Canada and Public Safety Canada.
6. NSIRA and the OPC recommend that federal institutions that routinely disclose or receive in accordance with the Act standardize their record keeping in accordance with the latest Public Safety guidance.
7. NSIRA and the OPC recommend that institutions ensure that records kept for bulk disclosures include an appropriately robust description of the information relied on to satisfy itself that the disclosure of all elements of the dataset meets section 5 of the Act, and that the level of internal oversight is commensurate with the privacy risk.
8. NSIRA and the OPC recommend that federal institutions include information about how the disclosure will contribute to their jurisdiction or responsibilities in respect of activities that

undermine the security of Canada, and other information relevant to the disclosure test, in their written requests for information under the Act, even if this information was verbally communicated prior to the request to enable appropriate record keeping by disclosing institutions under SCIDA.

9. NSIRA and the OPC recommend that IRCC and the CSE enter into an information-sharing arrangement that structures their disclosure of information under the Act.
10. NSIRA and the OPC recommend that CSIS and GAC update their information-sharing arrangement, previously agreed upon under SCISA, to account for SCIDA.
11. NSIRA and the OPC recommend that the Canadian Food Inspection Agency consult Public Safety Canada, and develop and implement policies and procedures to support compliance with the Act.

Annex B: Assessment of Core Policy elements by institutions

This annex tabulates the core policy elements that the 17 federal institutions listed in SCIDA have in place to support compliance with the Act.

The table shows what is in policy and not whether the institutions adhered to their policies and complied with the Act, as this is the focus of the rest of the report. For example, the Canadian Security Intelligence Service kept records of receipts of information under SCIDA and provided these to NSIRA, both of which are requirements under the Act, yet it has not yet set out this practice in policy.

Of the 17 federal institutions listed in the Act, the Canada Revenue Agency and the Canadian Security Intelligence Service cannot disclose information under the Act, so the first five policy elements do not apply to them.

The *Security of Canada Information Sharing Act* (SCISA) was in force from 2015 to 2019 and is the predecessor to SCIDA.

Federal institution that may receive information under the Act		Disclosing Institution				Record keeping and supporting independent review			
		The disclosing institution is satisfied that "the disclosure will contribute to the exercise of the recipient institution's jurisdiction, or the carrying out of its responsibilities, under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada"	The disclosing institution is satisfied that the "disclosure will not affect any person's privacy interest more than is reasonably necessary in the circumstances"	Statement regarding accuracy and reliability of the manner in which it was obtained	Sent to the deputy head or a designated person	Record keeping	Provision of records to NSIRA annually	Institution has fully updated its frameworks from SCISA to SCIDA	Total "Yes"
1	Canada Border Services Agency	Yes	Yes	Yes	Yes	Yes	Yes	No	7 of 8 core policy elements
2	Canada Revenue Agency	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	Yes	3 of 3 core policy elements
3	Canadian Food Inspection Agency	No	No	No	Yes	No	No	No	0 of 8 core policy elements
4	Canadian Security Intelligence Service	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Yes	Yes	No	2 of 3 core policy elements
5	Canadian Nuclear Safety Commission	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
6	Communications Security Establishment	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
7	Immigration, Refugees, and Citizenship Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements

8	Department of Finance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
9	Global Affairs Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
10	Health Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
11	National Defence	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
12	Canadian Armed Forces	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
13	Public Health Agency of Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
14	Public Safety Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
15	Transport Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
16	Financial Transactions and Reports Analysis Centre of Canada	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
17	Royal Canadian Mounted Police	Yes	Yes	Yes	Yes	Yes	Yes	Yes	8 of 8 core policy elements
Total "Yes"		14 of 15	14 of 15	14 of 15	14 of 15	16 of 17	16 of 17	14 of 17	

Annex C: NSIRA’s review of four disclosures of information made under SCIDA in 2019

Introduction

1. Given the challenges created by the COVID-19 pandemic and how it affected NSIRA’s work in 2020, the agency regrets that it was unable to review any disclosures of information made under SCIDA in 2019 in time for the publication in December 2020 of *NSIRA’s 2019 Annual Report on the Disclosure of Information under the Security of Canada Information Disclosure Act*. In that report, the agency committed to reviewing a small number of disclosures made in 2019 as a spot check, and to publishing the results in its 2020 SCIDA report.⁶³
2. This annex is that spot check.⁶⁴ This legal compliance review was based on the disclosures and receipts of information under SCIDA in 2019, and correspondence with the reviewed institutions in early 2021.

Authorities

3. NSIRA conducted this review under subsection 39(1) and paragraph 8(1)(b) of the *NSIRA Act*.

Findings and Recommendations

4. NSIRA reviewed four disclosures of information made in 2019 involving four federal institutions: the Canada Border Services Agency (CBSA); the Canadian Security Intelligence Service (CSIS); Immigration, Refugees and Citizenship Canada (IRCC); and, the Royal Canadian Mounted Police (RCMP). All four disclosures of information appear to have complied with SCIDA. Examples of two of the four disclosures are detailed below.

⁶³ National Security and Intelligence Review Agency, *NSIRA’s 2019 Annual Report on the Disclosure of Information under the Security of Canada Information Disclosure Act*, December 2020, <https://nsira-ossnr.ca/security-of-canada-information-disclosure-act>, para 3.

⁶⁴ As NSIRA’s 2019 Annual Report on the Disclosure of Information under the Security of Canada Information Disclosure Act was not coordinated with the OPC, the present annex was also not coordinated with the OPC.

DISCLOSURE #1: Immigration, Refugees and Citizenship Canada disclosed the contact information of an individual to the RCMP as the individual was a potential witness in a foreign law enforcement investigation

5. A foreign law enforcement agency asked the RCMP to locate an individual in Canada (the subject of the disclosure of information under SCIDA). The foreign law enforcement agency had informed the RCMP that the subject was a potential witness in their national security investigation, and that the foreign law enforcement agency wanted to conduct a witness interview with the subject.
6. In an effort to locate the subject, the RCMP asked IRCC for the subject's contact information contained in the subject's most recent passport application. IRCC disclosed the requested information.
7. NSIRA notes that IRCC aptly indicated that they did not add any information from the RCMP's request to the subject's passport file or "any kind of IRCC lookout or watchlist."⁶⁵ IRCC explains:

"IRCC solely uses the information [received by IRCC in requests for information under SCIDA] to assess the information sharing request. If IRCC comes across information in a request letter that it deems relevant to IRCC's mandate, the established practice is to disclose the information to IRCC separately under the appropriate info-sharing mechanism. This information would then be added to the subject's file for possible administrative action [by IRCC]."⁶⁶
8. This practice, while not verified by NSIRA, is encouraging because it helps ensure that information obtained by IRCC to fulfill its mandate is obtained under one of IRCC's legal authorities, and that requests for information received by IRCC do not become backhanded disclosures of information. Given the importance of this practice and that IRCC has "data on over an estimated 60 million foreign nationals, permanent residents and citizens"⁶⁷ and discloses large amounts of information under SCIDA and other authorities, this practice should be put into policy.

⁶⁵ Immigration, Refugees and Citizenship Canada, letter to NSIRA, 6 April 2021, p. 1.

⁶⁶ Immigration, Refugees and Citizenship Canada, letter to NSIRA, 6 April 2021, p. 1.

⁶⁷ Immigration, Refugees and Citizenship Canada, Immigration, Refugees and Citizenship Canada Policy on Information Sharing under the Security of Canada Information Disclosure Act, 12 May 2020, p. 2.

Recommendation no. 11: NSIRA recommends that Immigration, Refugees and Citizenship Canada and other institutions which routinely receive requests for information under SCIDA, put into written policy the practice of keeping information received in requests for information separate from the rest of its databanks and watch lists.

DISCLOSURE #2: Proactive disclosure of information from the Canada Border Services Agency to the Royal Canadian Mounted Police about an individual associated with an ideologically motivated violent extremist (IMVE) group

9. CBSA became aware that a foreign national (the subject of the disclosure) was associated with an IMVE group, and that the RCMP considered this violent extremist group an enforcement priority.
10. CBSA used SCIDA to proactively disclose information about the subject to the RCMP that CBSA had obtained during a secondary examination of the subject at a Port of Entry. NSIRA notes that disclosures of information under SCIDA should only be made to persons designated for this purpose, and that the RCMP has only designated persons at its National Headquarters in Ottawa.⁶⁸

⁶⁸ Public Safety Canada, SCIDA Step-by-Step Guide to Responsible Information Sharing, December 2019, p. 76.